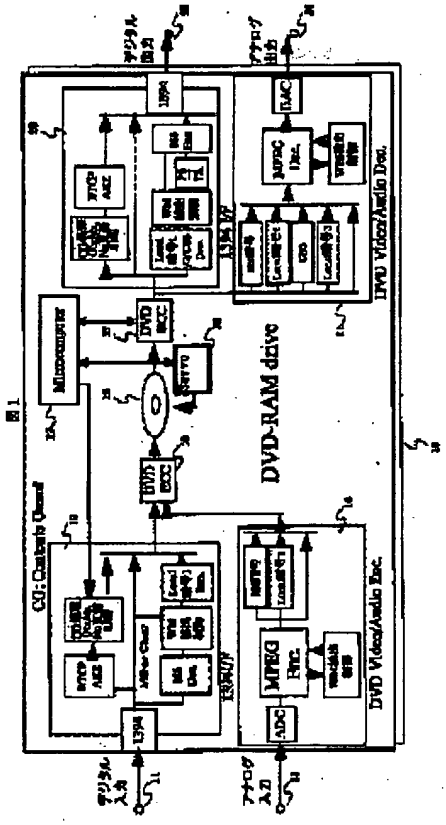
DATA RECORDER, DATA REPRODUCING DEVICE, DATA RECORDING METHOD AND DATA REPRODUCING METHOD

Patent number:	JP2001229614
Publication date:	2001-08-24
Inventor:	KAWAMAE OSAMU; NOGUCHI TAKAHARU; TAKEUCHI TOSHIFUMI
Applicant:	HITACHI LTD
Classification:	
- international:	G11B20/10; G06F12/14; G06T1/00; G09C5/00; H04N1/387; H04N5/91; H04N5/92
- european:	
Application number:	JP20000058962 20000303
Priority number(s):	JP20000058962 20000303; JP19990349162 19991208

Abstract not available for JP2001229614



(19)日本国特許庁(JP)　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開２００１－２２９６１４
(Ｐ２００１－２２９６１４Ａ)
(43)公開日　平成13年8月24日(2001.8.24)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
Ｇ１１Ｂ	20/10		Ｇ１１Ｂ	20/10	Ｈ	5B017
		３０１			３０１Ａ	5B057
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ	12/14	３２０Ｅ	5C053
Ｇ０６Ｔ	1/00	５００	Ｇ０６Ｔ	1/00	５００Ｂ	5C076
Ｇ０９Ｃ	5/00		Ｇ０９Ｃ	5/00		5D044

審査請求　未請求　請求項の数２０　ＯＬ　（全２６頁）　最終頁に続く

(21)出願番号　特願2000-58962(P2000-58962)

(22)出願日　平成12年3月3日(2000.3.3)

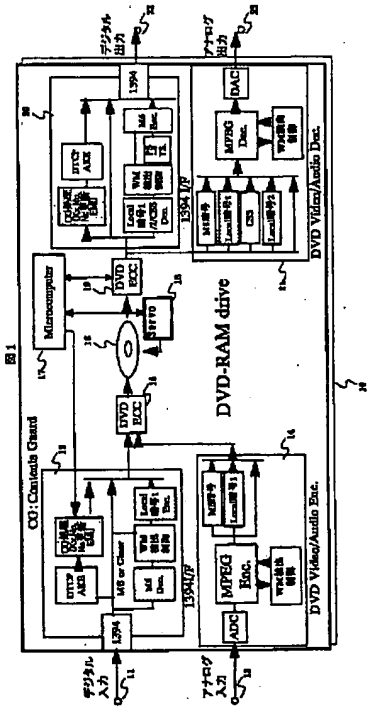
(31)優先権主張番号　特願平11-349162
(32)優先日　平成11年12月8日(1999.12.8)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(72)発明者　川前　治
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(72)発明者　竹内　敏文
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内
(74)代理人　100078134
弁理士　武　顕次郎

最終頁に続く

(54)【発明の名称】データ記録装置およびデータ再生装置およびデータ記録方法およびデータ再生方法

(57)【要約】
【課題】　著作権のあるデータが不正に記録あるいは再生されることを防止すること。
【解決手段】　ディジタル入出力及びアナログ入出力を備えたビットストリーム記録再生装置、またはＲＴＲＷ記録再生装置において、適切なWM検出制御手段と暗号のエンコード／デコードを備える。



1

【特許請求の範囲】

【請求項１】　ディジタルデータを入力する入力端子と、転送されたディジタルデータを受信するインターフェイス手段と、前記転送されたディジタルデータを記録媒体に記録するための記録処理を行う記録処理手段と、データを記録媒体に記録する記録手段とを、備えたデータ記録装置において、

前記インターフェイス手段は、

前記ディジタルデータが暗号化されている場合には、暗号を復号する復号手段と、

復号されたディジタルデータから電子透かし情報を検出する第１の検出手段と、

前記ディジタルデータを暗号化する第１の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項２】　請求項１において、

アナログ信号を入力する入力端子と、アナログ信号をディジタル信号に変換するＡＤ変換手段と、変換された前記ディジタル信号を圧縮する圧縮手段とを備え、

前記圧縮手段は、

電子透かし情報を検出する第２の検出手段と、

圧縮されたデータを暗号化する第２の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項３】　アナログ信号を入力する入力端子と、アナログ信号をディジタル信号に変換するＡＤ変換手段と、変換された前記ディジタル信号を圧縮する圧縮手段と、圧縮されたディジタル信号を記録媒体に記録するための記録処理を行う記録処理手段と、データを記録媒体に記録する記録手段とを、備えたデータ記録装置において、

前記圧縮手段は、

電子透かし情報を検出する第２の検出手段と、

圧縮されたデータを暗号化する第２の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項４】　請求項３において、

ディジタルデータを入力する入力端子と、転送されたディジタルデータを受信するインターフェイス手段とを備え、

前記インターフェイス手段は、

前記ディジタルデータが暗号化されている場合には、暗号を復号する復号手段と、

復号されたディジタルデータから電子透かし情報を検出する第１の検出手段と、

前記ディジタルデータを暗号化する第１の暗号手段とを、備えたことを特徴とするデータ記録装置。

【請求項５】　請求項４において、

前記第１の暗号手段と前記第２の暗号手段で同じ暗号化を行う場合には、前記第１の暗号手段と前記第２の暗号手段とを共通化することを特徴とするデータ記録装置。

【請求項６】　データを記録媒体から再生する再生手段と、記録媒体から読み出したデータの再生処理を行う再

2

生処理手段と、再生処理後のディジタルデータを送信するインターフェイス手段と、ディジタルデータを出力する出力端子とを、備えたデータ再生装置において、

前記インターフェイス手段は、

前記再生処理後のディジタルデータが暗号化されている場合には、暗号を復号する第１の復号手段と、

復号されたディジタルデータから電子透かし情報を検出する第１の検出手段と、

前記ディジタルデータを暗号化する第１の暗号手段とを、備えたことを特徴とするデータ再生装置。

【請求項７】　請求項６において、

再生処理されたデータを伸長する伸長手段と、ディジタル信号をアナログ信号に変換するＤＡ変換手段と、アナログ信号を出力する出力端子とを備え、

再生処理され伸長処理される前のディジタルデータが暗号化されている場合には、暗号を復号する第２の復号手段を備え、

前記伸長手段は、電子透かし情報を検出する第２の検出手段を、備えたことを特徴とするデータ再生装置。

【請求項８】　データを記録媒体から再生する再生手段と、記録媒体から読み出したデータの再生処理を行う再生処理手段と、再生処理されたデータを伸長する伸長手段と、ディジタル信号をアナログ信号に変換するＤＡ変換手段と、アナログ信号を出力する出力端子とを、備えたデータ再生装置において、

再生処理後のディジタルデータが暗号化されている場合には、暗号を復号する第２の復号手段を備え、

前記伸長手段は、電子透かし情報を検出する第２の検出手段を、備えたことを特徴とするデータ再生装置。

【請求項９】　請求項８において、

再生処理後のディジタルデータを送信するインターフェイス手段と、ディジタルデータを出力する出力端子とを備え、

前記インターフェイス手段は、

このインターフェイス手段に入力される再生処理後のディジタルデータが暗号化されている場合には、暗号を復号する第１の復号手段と、

復号されたディジタルデータから電子透かし情報を検出する第１の検出手段と、

前記ディジタルデータを暗号化する第１の暗号手段とを、備えたことを特徴とするデータ再生装置。

【請求項１０】　請求項７または９において、

前記第１の復号手段と前記第２の復号手段で同じ復号化を行う場合には、前記第１の復号手段と前記第２の復号手段を共通化することを特徴とするデータ再生装置。

【請求項１１】　データを入力し、前記データを記録するデータ記録方法において、

前記入力データに暗号がかけられている場合には、一旦暗号を復号して、前記入力データに含まれている付加情報を検出し、

この検出結果に従って、前記入力データの記録を制御し、再び、所定の方法で入力データを暗号化して、記録データとするようにしたことを特徴とするデータ記録方法。

【請求項１２】　請求項１１において、
前記入力データの復号は、前記付加情報を検出できるデータフォーマットまで復号するようにしたことを特徴とするデータ記録方法。

【請求項１３】　請求項１１において、
前記入力データに暗号がかけられていない場合は、前記入力データに含まれている付加情報を検出し、
この検出結果に従って、前記入力データの記録の制御を行い、必要に応じて、再び、所定の方法で入力データを暗号化して、記録データとするようにしたことを特徴とするデータ記録方法。

【請求項１４】　請求項１１において、
前記入力データは転送するためのデータ列フォーマットで構成されており、記録データは異なるデータ列フォーマットで記録するときには、前記復号を行って、再度暗号化を行うまでの間に、データ列フォーマットの変換を行うようにしたことを特徴とするデータ記録方法。

【請求項１５】　記録媒体からデータを再生し、再生データを出力するデータ再生方法において、
前記再生データに暗号がかけられている場合には、一旦暗号を復号して、前記再生データに含まれている付加情報を検出し、
この検出結果に従って、前記再生データの出力を制御し、再び、所定の方法で再生データを暗号化して、出力データとするようにしたことを特徴とするデータ再生方法。

【請求項１６】　請求項１５記載において、
前記再生データの復号は、前記付加情報を検出できるデータフォーマットまで復号するようにしたことを特徴とするデータ再生方法。

【請求項１７】　請求項１５記載において、
前記再生データに暗号がかけられていない場合は、前記再生データに含まれている付加情報を検出し、
この検出結果に従って、前記再生データの出力の制御を行い、必要に応じて、再び、所定の方法で再生データを暗号化して、出力データとするようにしたことを特徴とするデータ再生方法。

【請求項１８】　請求項１５記載において、
前記入力データは記録媒体に記録するためのデータ列フォーマットで構成されており、
出力データは異なるデータ列フォーマットで出力するときには、前記復号を行って、再度暗号化を行うまでの間に、データ列フォーマットの変換を行うようにしたことを特徴とするデータ再生方法。

【請求項１９】　請求項４において、
前記第１の検出手段と前記第２の検出手段を兼用したことを特徴とするデータ記録装置。

【請求項２０】　請求項９において、
前記第１の検出手段と前記第２の検出手段を兼用したことを特徴とするデータ再生装置。

【発明の詳細な説明】

【０００１】
【発明の属する技術分野】本発明は、画像や音声データを記録および／または再生する装置並びに方法に係り、特に、記録媒体の複写管理情報に応じて記録再生あるいは再生あるいは記録の動作を制御するようにした技術に関する。

【０００２】
【従来の技術】ＤＶＤ－ＲＯＭは、ＣＤ－Ｒの約７倍の容量を持つ媒体である。これにはＰＣ用のプログラムコードだけでなく、映像や音声データを圧縮することで映画ソフトを記録することもできる。ＤＶＤにデータを記録する記録媒体としては、ＤＶＤ－ＲＡＭや、ＤＶＤ－Ｒ、ＤＶＤ－ＲＷがある。これらにも大容量のデータを記録することが出来るため、映画などのソフトウェアがそのままディジタル複写されることを防止しなければならない。このため、不正複写防止技術が重要になる。

【０００３】この技術の一つとして、電子透かし技術があり、その標準化について日経ＢＰ社「日経エレクトロニクス」（1998.5.18 P31～P32）に記載されている。

【０００４】また、電子透かし技術とは別に、ＩＥＥＥ１３９４を使って機器間でのデータのやり取りにおける不正複写防止技術についても、日経ＢＰ社「日経エレクトロニクス」（1998.3.23 P47～P53）に記載されている。

【０００５】
【発明が解決しようとする課題】しかし、ＤＶＤ－ＲＡＭドライブのように、ディジタル／アナログ入出力を備えた機器については、これらの技術だけで不正複写を防止することは困難であり、また容易に回避されてしまうこともある。また、ＰＣ内部では、さらに複雑なデータのやり取りが行われるため、複写制御の抜け道も発生しやすくなる。

【０００６】このため、電子透かし技術やＩＥＥＥ１３９４複写防止技術も含めて、複数の複写制御技術を適切に組み合わせて用いるシステムを構築することが求められている。

【０００７】本発明は上記の点に鑑みなされたもので、その目的とするところは、ディジタル／アナログ入出力を備えたビットストリーム記録再生装置あるいはＲＴＲＷ記録再生装置において、著作権のあるデータが不正に記録または再生されることを防止することにある。

【０００８】
【課題を解決するための手段】上記目的を達成するために、本発明は、例えば、ディジタルデータを入力する入力端子と、転送されたディジタルデータを受信するイン

ターフェイス手段と、アナログ信号を入力する入力端子と、アナログ信号をディジタル信号に変換するＡＤ変換手段と、この変換されたディジタル信号を圧縮する圧縮手段と、前記転送されたディジタルデータと圧縮されたディジタル信号を記録媒体に記録するための記録処理を行う記録処理手段と、データを記録媒体に記録する記録手段とを、備えたデータ記録装置において、前記インターフェイス手段は、前記ディジタルデータが暗号化されている場合には、暗号を復号する復号手段と、復号されたディジタルデータから電子透かし情報を検出する第１の検出手段と、前記ディジタルデータを暗号化する第１の暗号手段とを備え、前記圧縮手段は、電子透かし情報を検出する第２の検出手段と、圧縮されたデータを暗号化する第２の暗号手段とを備える。

【０００９】また、本発明は、例えば、データを記録媒体から再生する再生手段と、記録媒体から読み出したデータの再生処理を行う再生処理手段と、再生処理後のディジタルデータを送信するインターフェイス手段と、ディジタルデータを出力する出力端子と、再生処理されたデータを伸長する伸長手段と、ディジタル信号をアナログ信号に変換するＤＡ変換手段と、アナログ信号を出力する出力端子とを、備えたデータ再生装置において、前記インターフェイス手段は、このインターフェイス手段に入力される再生処理後のディジタルデータが暗号化されている場合には、暗号を復号する第１の復号手段と、復号されたディジタルデータから電子透かし情報を検出する第１の検出手段と、前記ディジタルデータを暗号化する第１の暗号手段とを備え、また、再生処理され伸長処理される前のディジタルデータが暗号化されている場合には、暗号を復号する第２の復号手段を備え、前記伸長手段は、電子透かし情報を検出する第２の検出手段を備える。

【００１０】

【発明の実施の形態】以下、本発明の実施の形態を、図面を用いて説明する。

【００１１】図１は、本発明の１実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。本実施形態は、例えば、ＤＶＤ－ＲＡＭドライブのような記録再生を行う機器への適用例について示すが、本発明は、記録再生装置に限定されるものではなく、記録装置や再生装置にも適用されるものであって、本実施形態（および後述する実施形態）の記録再生装置には、記録装置や再生装置がその一部として含まれているものとして理解されたい。

【００１２】また、データ転送のインターフェース（以下、Ｉ／Ｆと記す）として、以下の説明では、ＩＥＥＥ１３９４を例にとるが、Ｉ／Ｆとしてはこれ以外にも、ＡＴＡＰＩやＳＣＳＩ、ＵＳＢなどが考えられ、Ｉ／Ｆの種別は特に限定されるものではない。また、本実施形態（および後述する実施形態）は、例えば、ＤＶＤ－ＲＡＭのような記録再生可能な媒体に記録再生を行う装置について示すが、記録媒体は光ディスクに限定されるものではなく、データを記録再生または再生する記録媒体全般にあてはまる。

【００１３】図１において、１０はビットストリーム（Bit-stream）記録再生可能なＤＶＤ－ＲＡＭドライブ、１１はディジタル入力端子、１２はＩＥＥＥ１３９４Ｉ／Ｆ、１３はアナログ入力端子、１４はＤＶＤビデオ／オーディオエンコーダ、１５はＤＶＤ誤り訂正符号付加手段、１６はＤＶＤディスク、１７はマイクロコンピュータ、１８はサーボ手段、１９はＤＶＤ誤り訂正手段、２０はＩＥＥＥ１３９４Ｉ／Ｆ、２１はＤＶＤビデオ／オーディオデコーダ、２２はディジタル出力端子、２３はアナログ出力端子である。

【００１４】次に、本実施形態の動作を説明する。

【００１５】ここではまず、動画や音声データを例えばＭＰＥＧ（Moving Picture ExpertsGroup）などの方式で圧縮し、ビットストリームデータ列で記録するＤＶＤ－ＲＡＭドライブの動作について説明する。ＤＶＤ－ＲＡＭドライブ１０への信号入力としては、ディジタル信号で入力される場合と、アナログ信号で入力される場合とがある。そのため、ＤＶＤ－ＲＡＭドライブ１０は、どちらの信号に対しても処理が可能なように処理手段を備える必要がある。それぞれの入力に対する動作を、図１とともに図２、３を用いて説明する。

【００１６】図２は、図１におけるＩＥＥＥ１３９４Ｉ／Ｆ１２の構成を示したものである。同図において、３１はＩＥＥＥ１３９４信号受信手段、３２はＤＴＣＰ（Digital Transmission Content Protection ）で採用された方式に則って複写制御を行うＤＴＣＰ手段、３３はＣＧ（Contents Guard）方式に則って複写制御を行うＣＧ処理手段、３４はＭ６暗号のデコード手段、３５はウォーターマーク（電子透かし；以下、ＷＭと記す）を検出し、それに従って制御するＷＭ検出制御手段、３６は所定の暗号化を行う暗号１エンコーダである。

【００１７】ＩＥＥＥ１３９４Ｉ／Ｆを介してディジタル入力で受け取った信号は、ＩＥＥＥ１３９４信号受信手段３１で受信され、転送データがとり出される。ＤＴＣＰ手段３２は、機器間認証、コピー制御伝送、コンテンツ暗号化により、ＩＥＥＥ１３９４バス上を伝送するコンテンツを保護するものであり、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行い、ＣＧ処理手段３３は、受信した鍵情報を更新し、新たな鍵情報を記録情報として記録する。

【００１８】ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で読み出すことができないようにしてある。ＩＥＥＥ１３９４ではＭ６暗号が採用されている。権利の無いものについては、暗号化されずクリアな信号として転送される。

【００１９】そのため、Ｍ６暗号がかかったデータはデコード手段３４によってＭ６暗号をデコードして、ＷＭ検出可能なデータとし、ＷＭ検出制御手段３５によりＷＭを検出し、検出結果にしたがって、出力を制御する。ＷＭ検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、暗号１エンコーダ３６により、所定の暗号化を行い、ＤＶＤ誤り訂正符号付加手段１５へ送る。ここで、暗号１はＭ６暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【００２０】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、ＷＭ検出を行うようにする。ＷＭが検出された場合には、ＷＭにしたがって制御され、必要に応じて、暗号１エンコーダ３６により、所定の暗号化を行い、ＤＶＤ誤り訂正符号付加手段１５へ送る。

【００２１】ＷＭ検出ではＤＶＤディスクに記録するために、コピー制御情報の更新が必要な場合には、ＷＭの更新を行ってから暗号化を行う。

【００２２】ＷＭ検出制御手段３５は、ＩＥＥＥ１３９４信号受信手段３１からの転送データに対してＷＭ検出を行うものである。このＷＭ検出が転送されたデータからそのまま検出が可能であれば、その状態から検出を行うが、例えば転送データがＭＰＥＧ圧縮によるビットストリームであるのに対して、ベースバンドの状態からの検出に対応したＷＭ検出であれば、一旦ビットストリームからベースバンドに変換してＷＭを検出し、その後に元の状態に逆変換して戻すようにする。ここで、変換するレベルは、完全にベースバンドまで変換しなくても、ＷＭ検出が可能な段階まで変換を行えば良い。この時に用いるＭＰＥＧエンコーダ・デコーダは、ＤＶＤビデオ／オーディオエンコーダ１４、ＤＶＤビデオ／オーディオデコーダ２１と兼用することも可能である。

【００２３】ここでは、ＭＰＥＧ圧縮変換について述べたが、ＷＭ検出するために必要があれば、ＷＭの検出方式に併せた変換もしくは変換の一部を行い、ＷＭ検出後にもとの状態に逆変換することにより、最適にＷＭ検出を行うことが可能となる。また、この変換はＷＭの書き換えや追加が必要な場合にも適応させることが出来る。

【００２４】図３は、図１におけるＤＶＤビデオ／オーディオエンコーダ１４の構成を示したものである。同図において、４１はＡＤコンバータ、４２はＭＰＥＧエンコーダ、４３はＷＭ検出制御手段、４４はＭ６暗号エンコーダ、４５は暗号２エンコーダである。

【００２５】映像信号や音声信号などのアナログ信号は、ＡＤコンバータ４１によりディジタル化される。ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されており、この信号が検出された場合には、コピーを禁止するように制御する。

【００２６】次に、ディジタル化されたデータはＭＰＥＧのような圧縮方式で圧縮される。同時にＷＭ検出制御４３により、ＷＭを検出し、ＷＭが検出された場合にはＷＭにしたがって制御される。ＷＭが検出されなかったり、データに権利が無いことを示すＷＭであった場合には、記録するデータを暗号化する必要はないので、ＭＰＥＧエンコードの後、そのままＤＶＤ誤り訂正符号付加手段１５へ送る。

【００２７】ＷＭ検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、Ｍ６暗号エンコーダ４４または暗号２エンコーダ４５により、所定の暗号化を行い、ＤＶＤ誤り訂正符号付加手段１５へ送る。

【００２８】ＷＭ検出ではＤＶＤディスクに記録するために、コピー制御情報の更新が必要な場合には、ＷＭの更新を行ってから暗号化を行う。ここで、暗号２はＭ６暗号またはＭ１暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【００２９】このように、図２、３で示したＩＥＥＥ１３９４Ｉ／Ｆ１２、および、ＤＶＤビデオ／オーディオエンコーダ１４からの出力を受け取り、図１のＤＶＤ誤り訂正符号付加手段１５において、誤り訂正のための符号を付加するとともに、ＤＶＤディスク１６に記録できるフォーマットに変換する。マイクロコンピュータ１７は、記録再生のためのシステム制御を行い、サーボ手段１８をコントロールして、ＤＶＤディスクの回転やアクセスを制御する。また、図２で示したＣＧ処理における鍵情報のやり取りも行う。

【００３０】再生時も、記録時と同様ディジタル出力系とアナログ出力系があり、それぞれの出力に対する動作を、図１とともに図４、５、６を用いて説明する。

【００３１】図４は、図１におけるＩＥＥＥ１３９４Ｉ／Ｆ２０の構成を示したものである。同図において、４１はＣＧ（Contents Guard）方式に則って複写制御を行うＣＧ処理手段、４２はＤＴＣＰで採用された方式に則って複写制御を行うＤＴＣＰ手段、４３はＭ６暗号のデコード手段、４４はＣＳＳ（Contents Scramble System）のデコード手段、４５は暗号１のデコード手段、４６は暗号２のデコード手段、４７はＷＭを検出し、それに従って制御するＷＭ検出制御手段、４８はプログラムストリームをトランスポートストリームに変換するＰＳ→ＴＳ変換手段、４９はＭ６暗号エンコーダ、５０はＩＥＥＥ１３９４信号受信手段である。

【００３２】ＤＶＤディスクから再生されたデータは、ＤＶＤ誤り訂正手段１９で復調及び誤り訂正され、ディジタル出力系とアナログ出力系へ送られる。

【００３３】ＣＧ処理手段４１は、データ中に含まれた鍵情報を更新し、新たな鍵情報を記録情報としてＤＴＣ

Ｐ手段４２へ送る。ＤＴＣＰ手段４２は、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行う。ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で取り出しても正しく読むことができないようにして転送する。権利の無いものについては、暗号化せずクリアな信号として転送する。

【００３４】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。ＤＶＤ－ＲＯＭディスクのデータには、ＣＳＳの暗号がかけられており、これに対応したデコーダ（デコード手段４４）が必要である。記録時には、ディジタル入力系とアナログ入力系で、Ｍ６暗号と暗号１、暗号２の３種の暗号があったため、これらの対応した３種のデコーダ（デコード手段４３、４５、４６）を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダによりＷＭ検出可能なデータまでデコードし、WM検出制御４７によりWMを検出し、検出結果にしたがって、出力を制御する。

【００３５】WM検出の結果、不正に記録されたデータでなく、データの転送が許可されているデータであるならば、Ｍ６暗号エンコーダ４９により暗号化を行い、ＩＥＥＥ１３９４信号受信手段５０へ送る。

【００３６】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、WMにしたがって制御され、必要に応じてＭ６暗号化を行い、ＩＥＥＥ１３９４信号受信手段５０へ送る。

【００３７】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【００３８】なお、ここでは、ＰＳ→ＴＳ変換手段４８はWM検出制御手段４７の後段で処理する例として示したが、ＰＳ→ＴＳ変換手段４８の処理の後にWM検出制御を行うようにしても構わない。すなわち、ＰＳ→ＴＳ変換処理とWM検出制御の順番は入れ替えることが可能である。例えば、図１４は図４の信号の流れの一部を入れ替えたものである。

【００３９】ここで、WM検出制御手段４７は、記録媒体からの再生データに対してWM検出を行うものである。このWM検出が再生されたデータからそのまま検出が可能であれば、その状態から検出を行うが、例えばＷＭ検出がトランスポートストリームや、プログラムストリームの状態のどちらかに対応したものであれば、ストリーム変換の適切な部分でWM検出を行うようにする。また、それらのストリームの中間レベルでWM検出が可能ならば、適切なレベルの信号を用いてWM検出を行うようにする。もちろん、一旦ストリームの変換を行い、WMを検出した後に再び元のトリームに変換しても構わない。また、図４にも示したように、ＰＳ→ＴＳ変換が必要ない場合には、変換を行わずにWM検出し、出力することも可能である。

【００４０】また、再生データがＭＰＥＧ圧縮によるビットストリームであるのに対して、ベースバンドの状態からの検出に対応したWM検出であれば、一旦ビットストリームからベースバンドに変換してWMを検出し、その後に元の状態に逆変換して戻すようにする。ここで、変換するレベルは、完全にベースバンドまで変換しなくても、WM検出が可能な段階まで変換を行えば良い。

【００４１】このように、WM検出が可能なレベルまでデータ状態を変換するための構成とすることにより、余分な回路の増加を防止することが出来る。ここでは、ＭＰＥＧ圧縮と転送ストリーム変換について述べたが、ＷＭ検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【００４２】ここで、転送するデータは、トランスポートストリーム（ＴＳ）とプログラムストリーム（ＰＳ）の２種類あり、データ転送に応じて、変換する必要がある。ＭＰＥＧ－２システムの２種のストリームの構成の違いを、図５に示す。トランスポートストリームは、１８８バイトの固定長パケットを単位として、誤りの発生し易いＡＴＭ通信やディジタル放送などに用いられる。プログラムストリームは、複数の可変長のＰＥＳパケットから構成される複数のパックからなり、ＣＤ－ＲＯＭや磁気テープなどの誤りが発生しにくいメディアに用いられる。

【００４３】このようにストリームの構成の違いがあるため、ＤＶＤディスクから再生されたストリームはＰＳであるが、転送するメディアによっては、ＰＳ→ＴＳ変換する必要がある。そのため、図４において、プログラムストリームをトランスポートストリームに変換するＰＳ→ＴＳ変換手段４８により、ストリームを変換してからＭ６暗号化を行い、ＩＥＥＥ１３９４信号受信手段５０へ送る。

【００４４】Ｍ６暗号をエンコードしたデータは、ＩＥＥＥ１３９４信号受信手段５０を介してディジタル出力端子２３から転送データとして出力される。

【００４５】図６は、図１におけるＤＶＤビデオ／オーディオデコーダ２１の構成を示したものである。同図において、５１はＭ６暗号のデコード手段、５２はＣＳＳのデコード手段、５３は暗号１のデコード手段、５４は暗号２のデコード手段、５５はＭＰＥＧデコーダ、５６はWM検出制御手段、５７はＤＡコンバータである。

【００４６】ＤＶＤディスク１６から再生されたデータは、ＤＶＤ誤り訂正手段１９で復調及び誤り訂正され、

ディジタル出力系とアナログ出力系へ送られる。

【００４７】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。ＤＶＤ－ＲＯＭディスクのデータには、ＣＳＳの暗号がかけられており、これに対応したデコーダ（デコード手段５２）が必要である。記録時には、ディジタル入力系とアナログ入力系で、Ｍ６暗号と暗号１、暗号２の３種の暗号があったため、これらの対応した３種のデコーダ（デコード手段５１、５３、５４）を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダにより復号され、ＭＰＥＧデコーダ５５により映像信号と音声信号にデコードされる。

【００４８】ここで、WM検出制御手段５６によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データの出力が許可されているデータであるならば、ＤＡコンバータ５７を介してアナログ出力端子２３から出力する。また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合にはWMにしたがって制御される。

【００４９】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【００５０】ここでは図示していないが、映像信号の場合には通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、ＤＡコンバータ５７によりディジタル化されたアナログ出力にも、同様にマクロビジョン信号を付加して、コピーを禁止するように制御する。

【００５１】ここで、図２、３、４、６の説明において、説明をわかりやすくするためWM検出制御手段を独立に示したが、記録系側においてWM検出制御手段３５とWM検出制御手段４３とを兼用することも可能であり、また、再生系側においてWM検出制御手段４７とWM検出制御手段５６とを兼用することも可能である。

【００５２】図７は、本発明の他の実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。

【００５３】同図において、７０はＲＴＲＷ（Real Time Read Write）フォーマットで記録再生可能なＤＶＤ－ＲＡＭドライブ、７１はディジタル入力端子、７２はＩＥＥＥ１３９４Ｉ／Ｆ、７３はアナログ入力端子、７４はＤＶＤビデオ／オーディオエンコーダ、７５はＤＶＤ誤り訂正符号付加手段、７６はＤＶＤディスク、７７はマイクロコンピュータ、７８はサーボ手段、７９はＤＶＤ誤り訂正手段、８０はＩＥＥＥ１３９４Ｉ／Ｆ、８１はＤＶＤビデオ／オーディオデコーダ、８２はディジタル出力端子、８３はアナログ出力端子である。

【００５４】次に、本実施形態の動作を説明する。

【００５５】ここではまず、動画や音声データを例えばＭＰＥＧなどの方式で圧縮し、ＲＴＲＷフォーマットに変換して記録するＤＶＤ－ＲＡＭドライブの動作について説明する。ＤＶＤ－ＲＡＭドライブ７０への信号入力としては、ディジタル信号で入力される場合と、アナログ信号で入力される場合とがある。そのため、ＤＶＤ－ＲＡＭドライブ７０は、どちらの信号に対しても処理が可能なように処理手段を備える必要がある。それぞれの入力に対する動作を、図７とともに図８、９を用いて説明する。

【００５６】図８は、図７におけるＩＥＥＥ１３９４Ｉ／Ｆ７２の構成を示したものである。同図において、８９はＩＥＥＥ１３９４信号受信手段、８２はＤＴＣＰで採用された方式に則って複写制御を行うＤＴＣＰ手段、８３はＣＧ方式に則って複写制御を行うＣＧ処理手段、８４はＭ６暗号のデコード手段、８５はWMを検出し、それに従って制御するWM検出制御手段、８６は所定の暗号化を行う暗号１エンコーダ、８７はトランスポートストリームをプログラムストリームに変換するＴＳ→ＰＳ変換手段である。

【００５７】ＩＥＥＥ１３９４Ｉ／Ｆを介してディジタル入力で受け取った信号は、ＩＥＥＥ１３９４信号受信手段８９で受信され、転送データがとり出される。ＤＴＣＰ手段８２は、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行い、ＣＧ処理手段８３は受信した鍵情報を更新し、新たな鍵情報を記録情報として記録する。

【００５８】ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で読み出すことができないようにしてある。ＩＥＥＥ１３９４ではＭ６暗号が採用されている。権利の無いものについては、暗号化されずクリアな信号として転送される。

【００５９】そのため、Ｍ６暗号がかかったデータはデコード手段８４によってＭ６暗号をデコードして、WM検出可能なデータとし、WM検出制御手段８５によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、ＴＳ→ＰＳ変換手段８７によりフォーマットの変換を行ない、その後、暗号１エンコーダ８６により、所定の暗号化を行い、ＤＶＤ誤り訂正符号付加手段７５へ送る。ここで、暗号１はＭ６暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【００６０】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここで、WMが検出された場合には、WMにしたがって制御され、必要に応じて、暗号１

エンコーダ３６により、所定の暗号化を行い、ＤＶＤ誤り訂正符号付加手段７５へ送る。

【００６１】WM検出では、ディスクに記録するためにコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。

【００６２】なお、ここではＴＳ→ＰＳ変換手段８７はWM検出制御手段８５の後段で処理する例として示したが、ＴＳ→ＰＳ変換手段８７の処理の後にWM検出制御を行なうようにしても構わない。すなわち、ＴＳ→ＰＳ変換処理とWM検出制御の順番は入れ替えることが可能である。例えば、図１５は図８の信号の流れの一部を入れ替えたものである。

【００６３】ここで、WM検出制御手段８５は、ＩＥＥＥ１３９４信号受信手段８９からの転送データに対してWM検出を行うものである。このWM検出が転送されたデータからそのまま検出が可能であれば、その状態から検出を行うが、例えばWM検出がトランスポートストリームや、プログラムストリームの状態のどちらかに対応したものであれば、ストリーム変換の適切な部分でWM検出を行うようにする。また、それらのストリームの中間レベルでWM検出が可能ならば、検出に適切なレベルの信号を用いてWM検出を行うようにする。もちろん、一旦ストリームの変換を行い、WMを検出した後に再び元のトリームに変換しても構わない。また、ＴＳ→ＰＳ変換が必要ない場合には、変換を行わずにWM検出し、出力することも可能である。

【００６４】また、再生データがＭＰＥＧ圧縮によるビットストリームであるのに対して、ベースバンドの状態からの検出に対応したWM検出であれば、一旦ビットストリームからベースバンドに変換してWMを検出し、その後に元の状態に逆変換して戻すようにする。ここで、変換するレベルは、完全にベースバンドまで変換しなくても、WM検出が可能な段階まで変換を行えば良い。

【００６５】このように、WM検出が可能なレベルまでデータ状態を変換するための構成とすることにより、余分な回路の増加を防止することが出来る。ここでは、ＭＰＥＧ圧縮と転送ストリーム変換について述べたが、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【００６６】このようにデータの変換や暗号の復号・符号化は、ここ示した順序のみでなく、処理順序を入れ替えることも可能であるため、この順序に限定されるものではない。また、ここでは、転送ストリーム変換について述べたが、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【００６７】図９は、図７におけるＤＶＤビデオ／オーディオエンコーダ７４の構成を示したものである。同図において、９１はＡＤコンバータ、９２はＭＰＥＧエンコーダ、９３はWM検出制御手段、９４はＭ６暗号エンコーダ、９５は暗号２エンコーダである。

【００６８】映像信号や音声信号などのアナログ信号は、ＡＤコンバータ９１によりディジタル化される。ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されており、この信号が検出された場合には、コピーを禁止するように制御する。

【００６９】次に、ディジタル化されたデータはＭＰＥＧのような圧縮方式で圧縮される。

【００７０】同時にWM検出制御手段９３により、WMを検出し、WMが検出された場合にはWMにしたがって制御される。WMが検出されなかったり、データに権利が無いことを示すWMであった場合には、記録するデータを暗号化する必要はないので、ＭＰＥＧエンコードの後、そのままＤＶＤ誤り訂正符号付加手段７５へ送る。

【００７１】WM検出の結果、不正にコピーしたデータでなく、記録媒体への記録が許可されているデータであるならば、Ｍ６暗号エンコーダ９４または暗号２エンコーダ９５により、所定の暗号化を行い、ＤＶＤ誤り訂正符号付加手段７５へ送る。WM検出では、ディスクに記録するためにコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。ここで、暗号２はＭ６暗号またはＭ１暗号と同じ暗号を用いても構わない。同じ暗号を用いることで、暗号の復号回路も共通化が図れるため、回路を簡略することができる。

【００７２】このように、図８、９で示したＩＥＥＥ１３９４Ｉ／Ｆ７２、および、ＤＶＤビデオ／オーディオエンコーダ７４からの出力を受け取り、図７のＤＶＤ誤り訂正符号付加手段７５において、誤り訂正のための符号を付加するとともに、ＤＶＤディスク７６に記録できるフォーマットに変換する。マイクロコンピュータ７７は、記録再生のためのシステム制御を行い、サーボ手段７８をコントロールして、ＤＶＤディスクの回転やアクセスを制御する。また、図８で示したＣＧ処理における鍵情報のやり取りも行う。

【００７３】再生時も、記録時と同様ディジタル出力系とアナログ出力系があり、それぞれの出力に対する動作を、図７とともに図１０、１１を用いて説明する。

【００７４】図１０は、図７におけるＩＥＥＥ１３９４Ｉ／Ｆ７０の構成を示したものである。同図において、１０１はＣＧ（Contents Guard）方式に則って複写制御を行うＣＧ処理手段、１０２はＤＴＣＰで採用された方式に則って複写制御を行うＤＴＣＰ手段、１０３はＭ６暗号のデコード手段、１０４はＣＳＳ（Contents Scram

ble System）のデコード手段、１０５は暗号１のデコード手段、１０６は暗号２のデコード手段、１０７はWMを検出し、それに従って制御するWM検出制御手段、１０８はプログラムストリームをトランスポートストリームに変換するＰＳ→ＴＳ変換手段、１０９はＭ６暗号エンコーダ、１１０はＩＥＥＥ１３９４信号受信手段である。

【００７５】ＤＶＤディスクから再生されたデータは、ＤＶＤ誤り訂正手段７９で復調及び誤り訂正され、ディジタル出力系とアナログ出力系へ送られる。

【００７６】ＣＧ処理手段１０１は、データ中に含まれた鍵情報を更新し、新たな鍵情報を記録情報としてＤＴＣＰ手段１０２へ送る。ＤＴＣＰ手段１０２は、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行う。ここで、転送データに著作権のような権利があるものは、暗号をかけることによりデータを転送途中で取り出しても正しく読むことができないようにして転送する。

【００７７】権利の無いものについては、暗号化せずクリアな信号として転送する。

【００７８】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。ＤＶＤ－ＲＯＭディスクのデータには、ＣＳＳの暗号がかけられており、これに対応したデコーダ（デコード手段１０４）が必要である。記録時には、ディジタル入力系とアナログ入力系で、Ｍ６暗号と暗号１、暗号２の３種の暗号があったため、これらの対応した３種のデコーダ（デコード手段１０３、１０５、１０６）を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダによりWM検出可能なデータまでデコードし、WM検出制御手段１０７によりWMを検出し、検出結果にしたがって、出力を制御する。

【００７９】WM検出の結果、不正に記録されたデータでなく、データの転送が許可されているデータであるならば、プログラムストリームをトランスポートストリームに変換するＰＳ→ＴＳ変換手段１０８により、ストリームを変換してから、Ｍ６暗号エンコーダ１０９により暗号化を行い、ＩＥＥＥ１３９４信号受信手段１１０へ送る。

【００８０】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、WMにしたがって制御され、ＰＳ→ＴＳ変換手段１０８により、ストリームを変換してから、必要に応じてＭ６暗号化を行い、ＩＥＥＥ１３９４信号受信手段１１０へ送る。

【００８１】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【００８２】なおここでも、図４で先に説明したのと同様に、ＰＳ→ＴＳ変換処理とWM検出制御の順番は入れ替えることが可能であり、図１４のように信号の流れの一部を入れ替えることが可能である。

【００８３】このように、WM検出するために必要があれば、WMの検出方式に併せた変換もしくは変換の一部を行い、WM検出後にもとの状態に逆変換することにより、最適にWM検出を行うことが可能となる。また、この変換はWMの書き換えや追加が必要な場合にも適応させることが出来る。

【００８４】図１１は、図７におけるＤＶＤビデオ／オーディオデコーダ８１の構成を示したものである。同図において、１１１はＭ６暗号のデコード手段、１１２はＣＳＳのデコード手段、１１３は暗号１のデコード手段、１１４は暗号２のデコード手段、１１５はＭＰＥＧデコーダ、１１６はWM検出制御手段、１１７はＤＡコンバータである。

【００８５】ＤＶＤディスクから再生されたデータは、ＤＶＤ誤り訂正手段７９で復調及び誤り訂正され、ディジタル出力系とアナログ出力系へ送られる。

【００８６】誤り訂正後のデータは暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。ＤＶＤ－ＲＯＭディスクのデータには、ＣＳＳの暗号がかけられており、これに対応したデコーダ（デコード手段１１２）が必要である。記録時には、ディジタル入力系とアナログ入力系で、Ｍ６暗号と暗号１、暗号２の３種の暗号があったため、これらの対応した３種のデコーダ（デコード手段１１１、１１３、１１４）を記したが、仮にこれらが同じ暗号を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダにより復号され、ＭＰＥＧデコーダ１１５により映像信号と音声信号にデコードされる。

【００８７】ここで、WM検出制御手段１１６によりWMを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データの出力が許可されているデータであるならば、ＤＡコンバータ１１７を介してアナログ出力端子７３から出力する。また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合にはWMにしたがって制御される。

【００８８】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【００８９】ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、ＤＡコンバータ１１７によりディジタル化されたアナログ出力にも、同様にマクロビ

ジョン信号を付加して、コピーを禁止するように制御する。

【００９０】このように、ディジタル入出力端子とアナログ入出力端子を備える記録再生装置で、データにかけられた暗号に対応して、適切な復号手段とWM検出制御手段を備えることにより、ディジタルデータ及びアナログデータのどちらに対しても適切なコピー制御を行うことが可能となる。なお、前述した２つの実施形態では、ディジタル入出力端子とアナログ入出力端子の両方を備えた機器として示したが、夫々単独での組み合わせも可能である。

【００９１】ここで、図８、９、１０、１１の説明において、説明をわかりやすくするためWM検出制御手段を独立に示したが、記録系側においてWM検出制御手段８５とWM検出制御手段９３とを兼用することも可能であり、また、再生系側においてWM検出制御手段１０７とWM検出制御手段１１６とを兼用することも可能である。

【００９２】図１２は、ＤＶＤビデオ／オーディオデコーダの別の例を示したものであり、本例は、ＰＣに接続されるビデオ／オーディオボードへの適用例である。

【００９３】図１２において、１１８はディジタル入力端子、１１９はアナログ出力端子、１２０はＰＣ用ビデオ／オーディオボード、１２１はＰＣ内部バスのインターフェイス、１２２は認証、及び鍵情報の受け渡しを行う認証手段、１２３はＭ６暗号のデコード手段、１２４はＣＳＳのデコード手段、１２５は暗号１のデコード手段、１２６は暗号２のデコード手段、１２７はＭＰＥＧデコーダ、１２８はWM検出制御手段、１２９はＤＡコンバータである。

【００９４】ＤＶＤドライブなどにより再生されたディジタルデータは、ＰＣに接続されるＭＰＥＧビデオ／オーディオボードに送られ、映像信号はモニタに出力され、音声信号はスピーカから出力される。

【００９５】ＰＣ内部バスのインターフェイス１２１は、例えばＰＣＩのようにＰＣ内部で、ボード間を接続するバスであったり、ＳＣＳＩやＡＴＡＰＩ、ＵＳＢのように外部の機器との接続のためのデータ転送インターフェイスであったり、特に限定はしない。

【００９６】データ転送を行うためには、認証手段１２２により接続する相手を確認し、鍵情報の受け渡しを行う。転送されるディジタルデータに、暗号がかかっている場合には、暗号化された方式に従ってデコードを行う。ＤＶＤ－ＲＯＭディスクのデータには、ＣＳＳの暗号がかけられており、これに対応したデコーダ（デコード手段１２４）が必要である。ＤＶＤディスクに記録するには、Ｍ６暗号と暗号１、暗号２の３種の暗号が考えられるため、これらの対応した３種のデコーダ（デコード手段１２３、１２５、１２６）を記してある。ここでは、３種のデコーダを別別に示したが、仮にこれらが同じ暗号方式を用いて記録されている場合には、それに対応してデコーダは兼用できる。各デコーダにより復号され、ＭＰＥＧデコーダ１２７により映像信号と音声信号にデコードされる。

【００９７】ここで、WM検出制御手段１２８によりＷＭを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データのアナログ出力が許可されているデータであるならば、ＤＡコンバータ１２９を介してアナログ出力端子１１９から出力する。

【００９８】また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、WMにしたがって制御される。WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。仮に、記録時にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【００９９】ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、ＤＡコンバータ１１７によりディジタル化されたアナログ出力にも、同様にマクロビジョン信号を付加して、コピーを禁止するように制御する。

【０１００】図１３は、ＩＥＥＥ１３９４Ｉ／Ｆを備えたＳＴＢ（Set Top Box ）の構成の１例を示したものである。

【０１０１】図１３において、１３０はＳＴＢ、１３１はディジタル入力端子、１３２はＩＥＥＥ１３９４信号受信手段、１３３はＤＴＣＰで採用された方式に則って複写制御を行うＤＴＣＰ手段、１３４はＣＧ方式に則って複写制御を行うＣＧ処理手段、１３５はＭ６暗号のデコード手段、１３６はＭＰＥＧデコーダ、１３７はWMを検出し、それに従って制御するWM検出制御手段、１３８はＤＡコンバータ、１３９はアナログ出力端子である。

【０１０２】ＳＴＢ１３０は、例えば図１に示したようなＤＶＤ記録再生装置から、ＩＥＥＥ１３９４を介してディジタルデータを受け取る。ＩＥＥＥ１３９４信号受信手段１３２で受信された転送データは、ＤＴＣＰ手段１３３により、データ転送を行う機器間での相互の認証と暗号を解くための鍵情報の受け渡しを行い、ＣＧ処理手段１３４は、受信した鍵情報を更新し、新たな鍵情報を記録情報として記録する。

【０１０３】ここで、転送データで著作権のような権利があるデータは、暗号をかけることによりデータを転送途中で読み出すことができないようにしてあり、ＩＥＥＥ１３９４ではＭ６暗号が採用されている。権利の無いものについては、暗号化されずクリアな信号として転送される。

【０１０４】そのため、Ｍ６暗号がかかったデータはＭ

６暗号をデコードして、映像や音声信号としてデコードできるようにする。ＭＰＥＧデコーダ１３６は、復号されたデータを映像信号と音声信号にデコードする。

【０１０５】ここで、WM検出制御手段１３７によりＷＭを検出し、検出結果にしたがって、出力を制御する。WM検出の結果、不正に記録されたデータでなく、データの出力が許可されているデータであるならば、ＤＡコンバータ１３８を介してアナログ出力端子１３９から出力する。また、暗号がかかっていないデータについても、不正にコピーされた可能性があるため、WM検出を行うようにする。ここでWMが検出された場合には、ＷＭにしたがって制御される。

【０１０６】WM検出ではコピー制御情報の更新が必要な場合には、WMの更新を行ってから暗号化を行う。既にWMの更新が既に行われていて、再生時に必要が無ければ更新は行わない。

【０１０７】ここでは図示していないが、映像信号の場合には、通常、マクロビジョン信号と呼ばれるコピー防止信号が付加されるため、ＤＡコンバータ１３８によりディジタル化されたアナログ出力にも、同様にマクロビジョン信号を付加して、コピーを禁止するように制御する。

【０１０８】なお、図１２、１３では、ディジタル入力でアナログ出力を備えた装置の例を示したが、入出力の組み合わせはこれらに限定されることはなく、また、複数の入出力を備えることも可能である。

【０１０９】このように、ディジタル入出力端子とアナログ入出力端子を備える記録再生装置で、データにかけられた暗号に対応して、適切な復号手段とWM検出制御手段を備えることにより、ディジタルデータ及びアナログデータのどちらに対しても適切なコピー制御を行うことが可能となる。

【０１１０】

【発明の効果】以上のように本発明によれば、ディジタル入出力及びアナログ入出力を備えたビットストリーム記録再生装置またはＲＴＲＷ記録再生装置などにおいて、適切なWM検出制御手段と暗号のエンコード／デコードを備えることにより、著作権のあるデータが不正に記録あるい再生されることを防止できる。

【図面の簡単な説明】

【図１】本発明の１実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。

【図２】図１のＩＥＥＥ１３９４Ｉ／Ｆ１２の構成例を示すブロックである。

【図３】図１のＤＶＤビデオ／オーディオエンコーダ１４の構成例を示すブロック図である。

【図４】図１のＩＥＥＥ１３９４Ｉ／Ｆ２０の構成例を示すブロック図である。

【図５】ＭＰＥＧ－２システムの２種のストリームの構成の違いを示す説明図である。

【図６】図１のＤＶＤビデオ／オーディオエンコーダ２１の構成例を示すブロック図である。

【図７】本発明の他の実施形態に係る、複写制御情報を含むデータを記録再生する記録再生装置の構成を示すブロック図である。

【図８】図７のＩＥＥＥ１３９４Ｉ／Ｆ７２の構成例を示すブロック図である。

【図９】図７のＤＶＤビデオ／オーディオエンコーダ７４の構成例を示すブロック図である。

【図１０】図７のＩＥＥＥ１３９４Ｉ／Ｆ８０の構成例を示す説明図である。

【図１１】図７のＤＶＤビデオ／オーディオエンコーダ８１の構成例を示すブロック図である。

【図１２】本発明のさらに他の実施形態に係る、再生出力系のＤＶＤビデオ／オーディオデコーダの構成例を示すブロック図である。

【図１３】本発明のさらに他の実施形態に係る、ＩＥＥＥ１３９４Ｉ／Ｆを備えたＳＴＢの構成の１例を示したブロック図である。

【図１４】図４のＩＥＥＥ１３９４Ｉ／Ｆ２０または図１０のＩＥＥＥ１３９４Ｉ／Ｆ７０の他の構成例を示すブロック図である。

【図１５】図８のＩＥＥＥ１３９４Ｉ／Ｆ７２の他の構成例を示すブロック図である。

【符号の説明】

１０　ビットストリーム記録再生可能なＤＶＤ－ＲＡＭドライブ
１１　ディジタル入力端子
１２　ＩＥＥＥ１３９４Ｉ／Ｆ
１３　アナログ入力端子
１４　ＤＶＤビデオ／オーディオエンコーダ
１５　ＤＶＤ誤り訂正符号付加手段
１６　ＤＶＤディスク
１７　マイクロコンピュータ
１８　サーボ手段
１９　ＤＶＤ誤り訂正手段
２０　ＩＥＥＥ１３９４Ｉ／Ｆ
２１　ＤＶＤビデオ／オーディオデコーダ
２２　ディジタル出力端子
２３　アナログ出力端子

【図１】

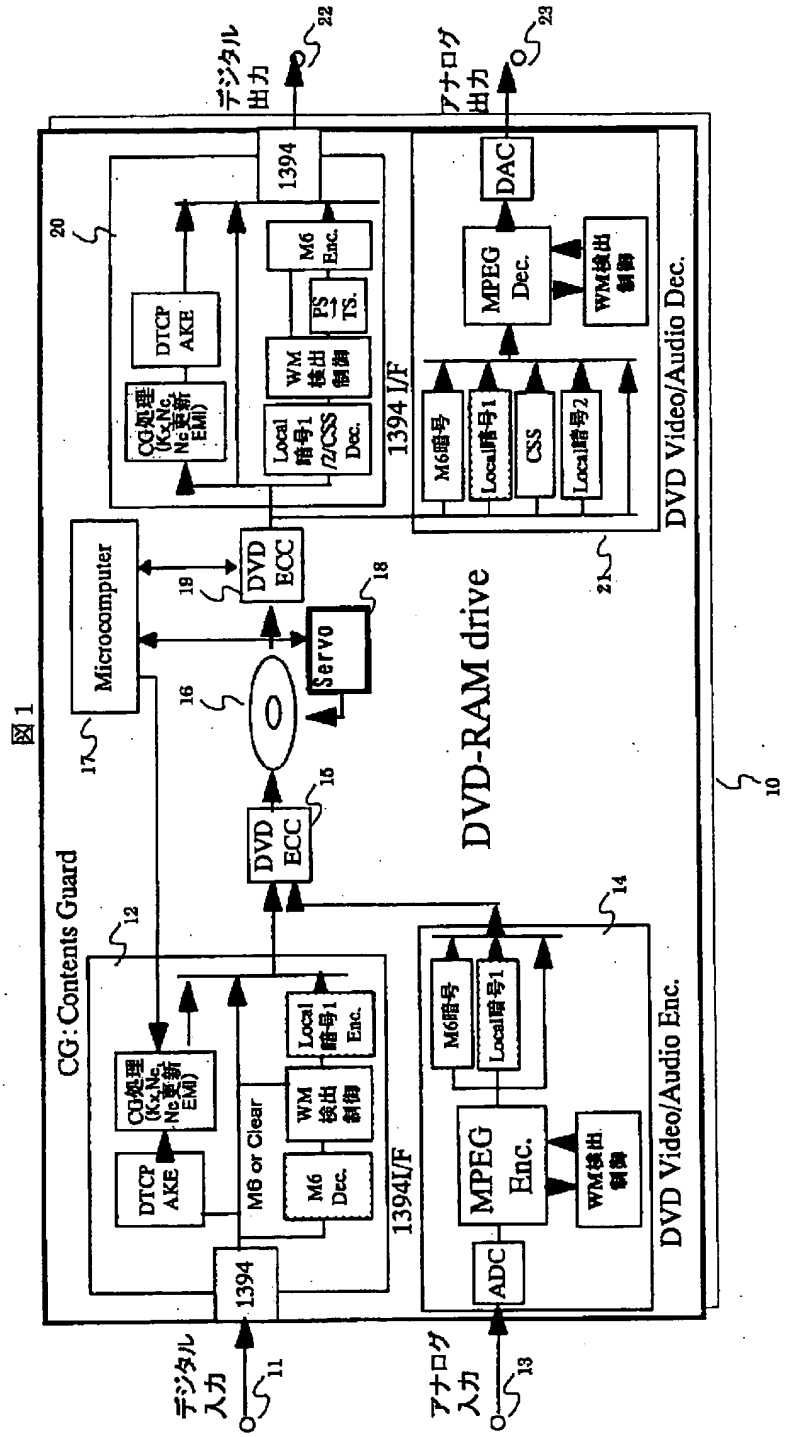
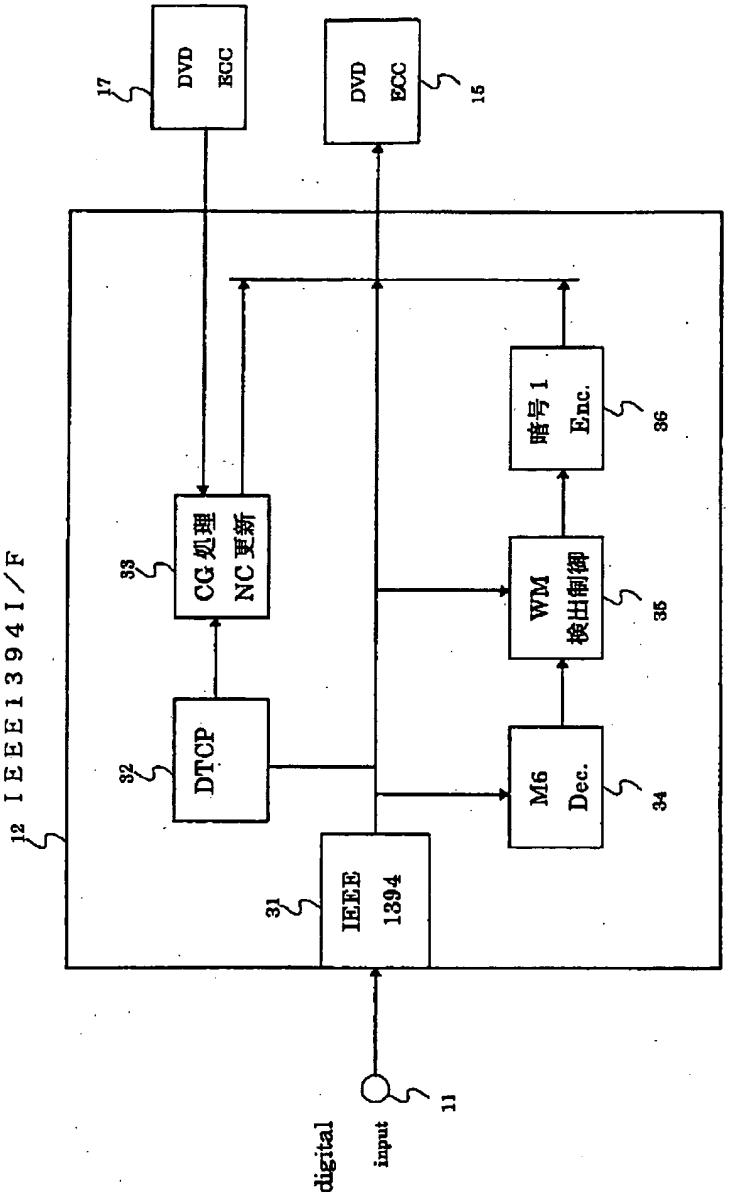


図１
CG:Contents Guard
DVD-RAM drive
DVD Video/Audio Enc.
DVD Video/Audio Dec.
Microcomputer
Servo
DVD ECC
DVD ECC
1394
1394
1394I/F
1394 I/F
DTCP AKE
CG処理 (Ks,Nc, Nc更新 EMI)
M6 or Clear
M6 Dec.
WM 検出 制御
Local 暗号1 Enc.
MPEG Enc.
ADC
M6暗号
Local暗号1
WM検出 制御
DTCP AKE
CG処理 (Ks,Nc, Nc更新 EMI)
M6 Enc.
PS → TS.
WM 検出 制御
Local 暗号1 /2/CSS Dec.
MPEG Dec.
DAC
M6暗号
Local暗号1
CSS
Local暗号2
WM検出 制御
デジタル 入力
アナログ 入力
デジタル 出力
アナログ 出力
10
11
12
13
14
15
16
17
18
18
20
21
22
23

【図2】

図2


digital input
11
IEEE 1394
31
IEEE1394I/F
12
DTCP
32
CG処理 NC更新
33
M6 Dec.
34
WM 検出制御
35
暗号1 Enc.
36
DVD ECC
15
DVD ECC
17

【図3】

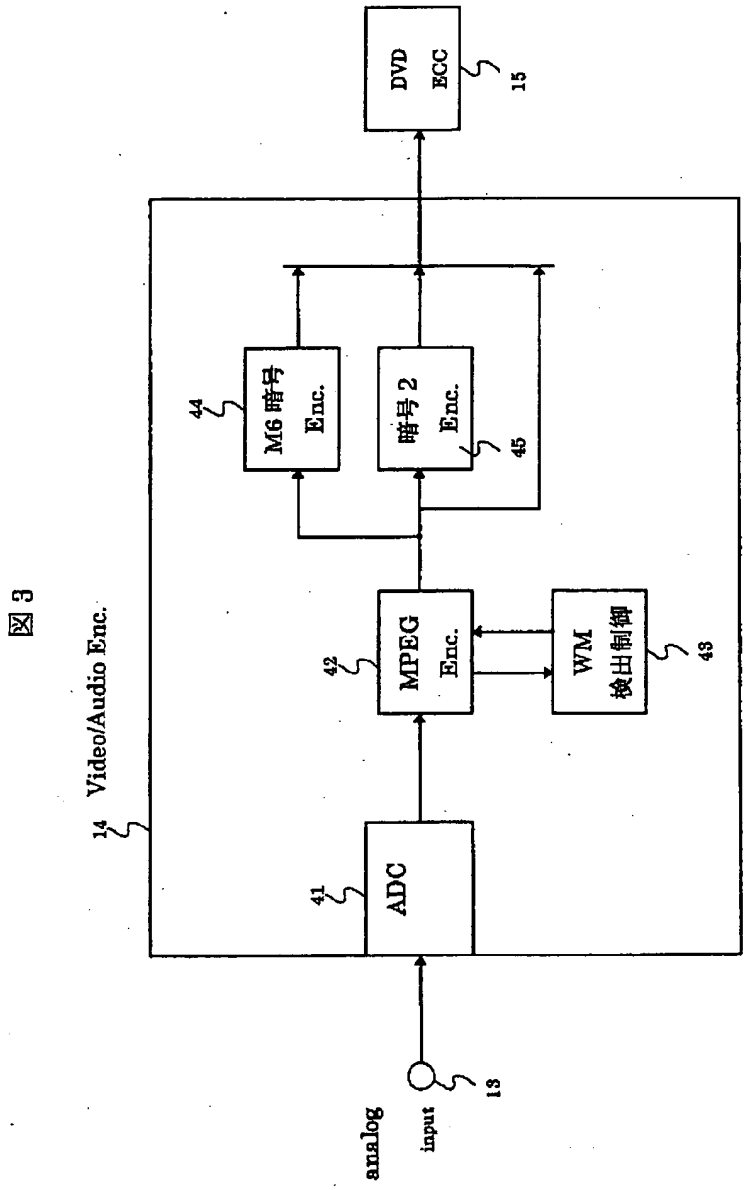

DVD
ECC
15
M6 暗号
Enc.
44
暗号 2
Enc.
45
MPEG
Enc.
42
WM
検出制御
43
ADC
41
14 Video/Audio Enc.
analog
input
13

図 3

【図4】

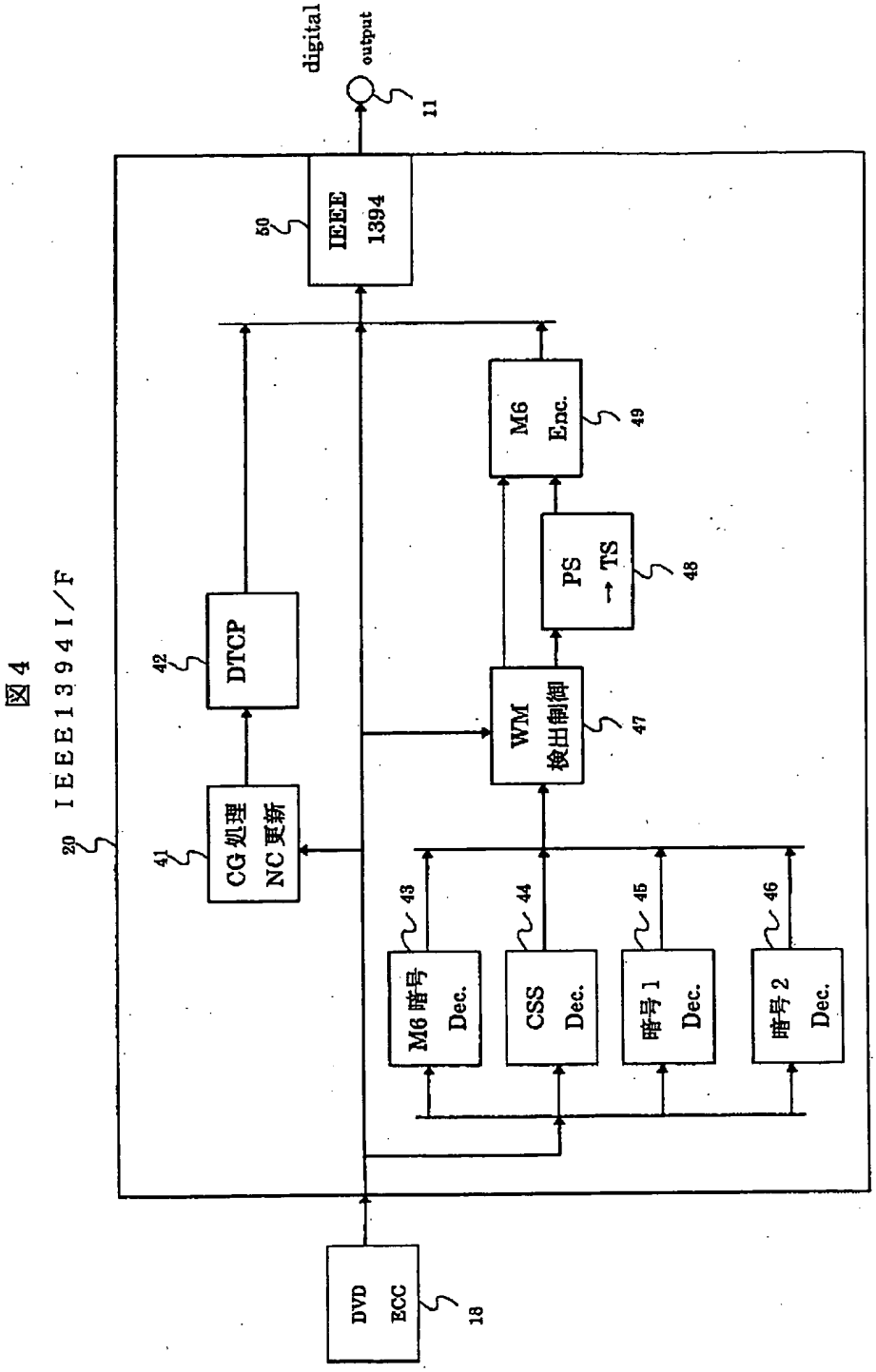
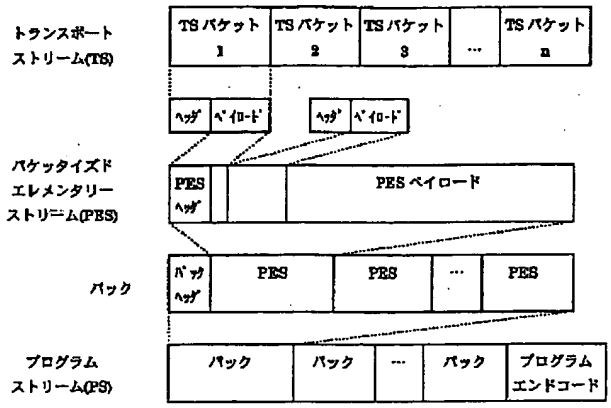

digital
output
11
50
IEEE
1394
M6
Enc.
49
PS
→ TS
48
WM
検出制御
47
42
DTCP
41
CG 処理
NC 更新
20
IEEE1394I/F
43
M6 暗号
Dec.
44
CSS
Dec.
45
暗号 1
Dec.
46
暗号 2
Dec.
DVD
ECC
18

図4

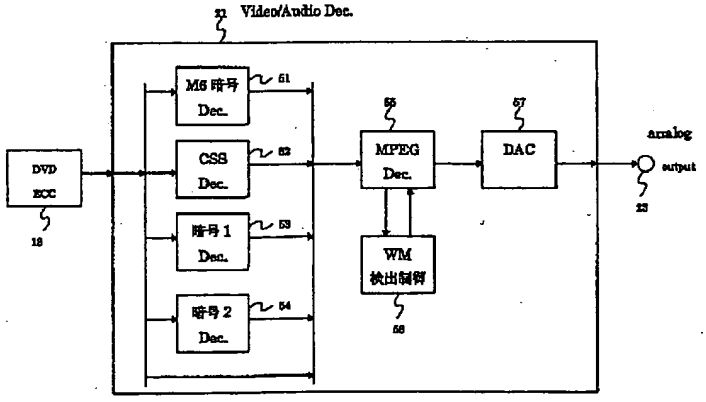
【図５】

図５


トランスポート
ストリーム(TS)
TS パケット 1
TS パケット 2
TS パケット 3
…
TS パケット n
ヘッダ
ペイロード
パケッタイズド
エレメンタリー
ストリーム(PES)
PES ヘッダ
PES ペイロード
パック
パック ヘッダ
PES
プログラム
ストリーム(PS)
パック
プログラム エンドコード

【図６】

図６


21
Video/Audio Dec.
M6 暗号 Dec.
61
CSS Dec.
62
暗号 1 Dec.
63
暗号 2 Dec.
64
DVD ECC
18
55
MPEG Dec.
57
DAC
analog output
23
WM 検出制御
56

【図7】

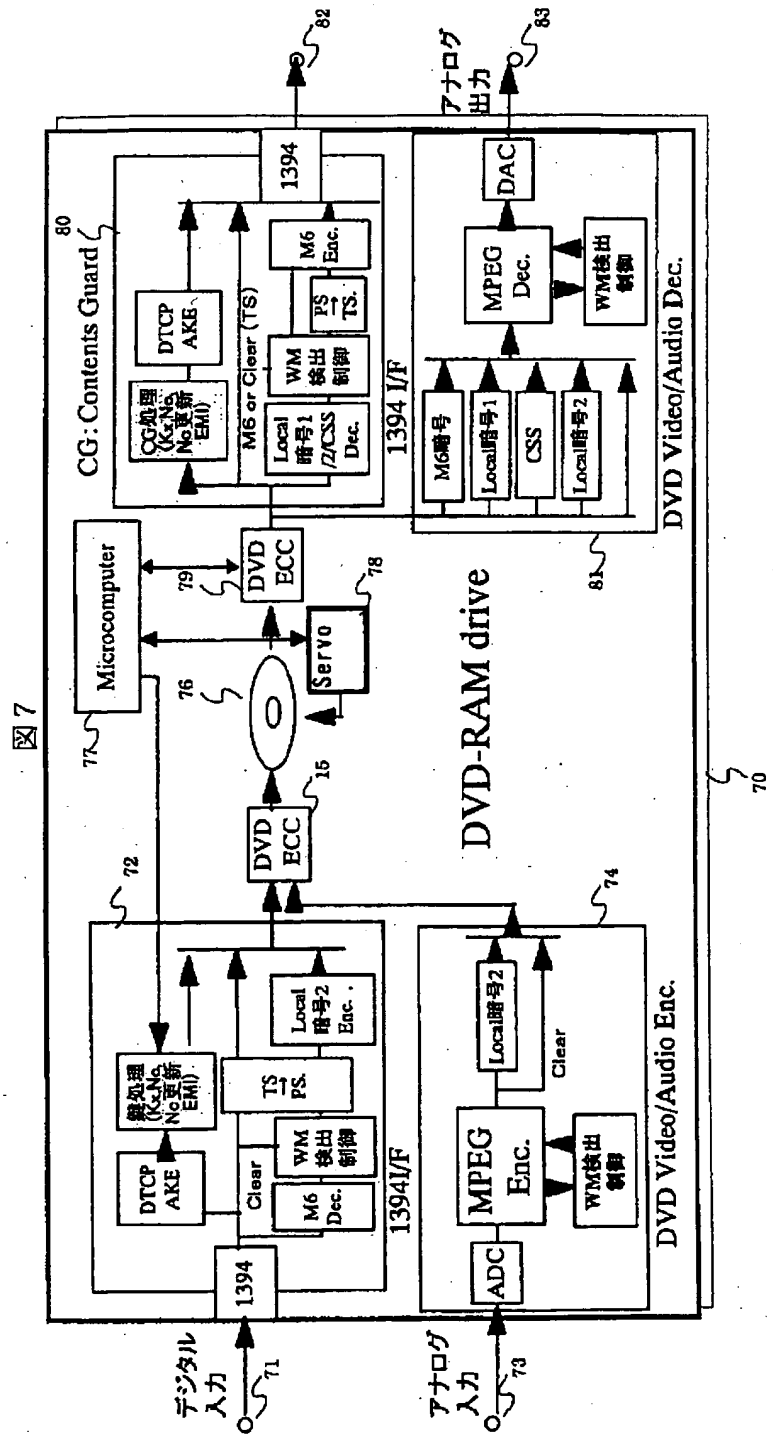


図7
DVD-RAM drive
70
CG: Contents Guard
80
1394
82
アナログ出力
83
DAC
MPEG Dec.
WM検出制御
M6暗号
Local暗号1
CSS
Local暗号2
DVD Video/Audio Dec.
81
1394 I/F
M6 Enc.
TS↑PS.
DTCP AKE
WM検出制御
M6 or Clear (TS)
CG処理 (Kc,No, No更新 EMI)
Local暗号1/2/CSS Dec.
Microcomputer
77
DVD ECC
79
Servo
78
76
15
72
74
1394I/F
Local暗号2 Enc.
TS↑PS.
WM検出制御
M6 Dec.
Clear
MPEG Enc.
ADC
DVD Video/Audio Enc.
デジタル入力
71
アナログ入力
73

【図8】

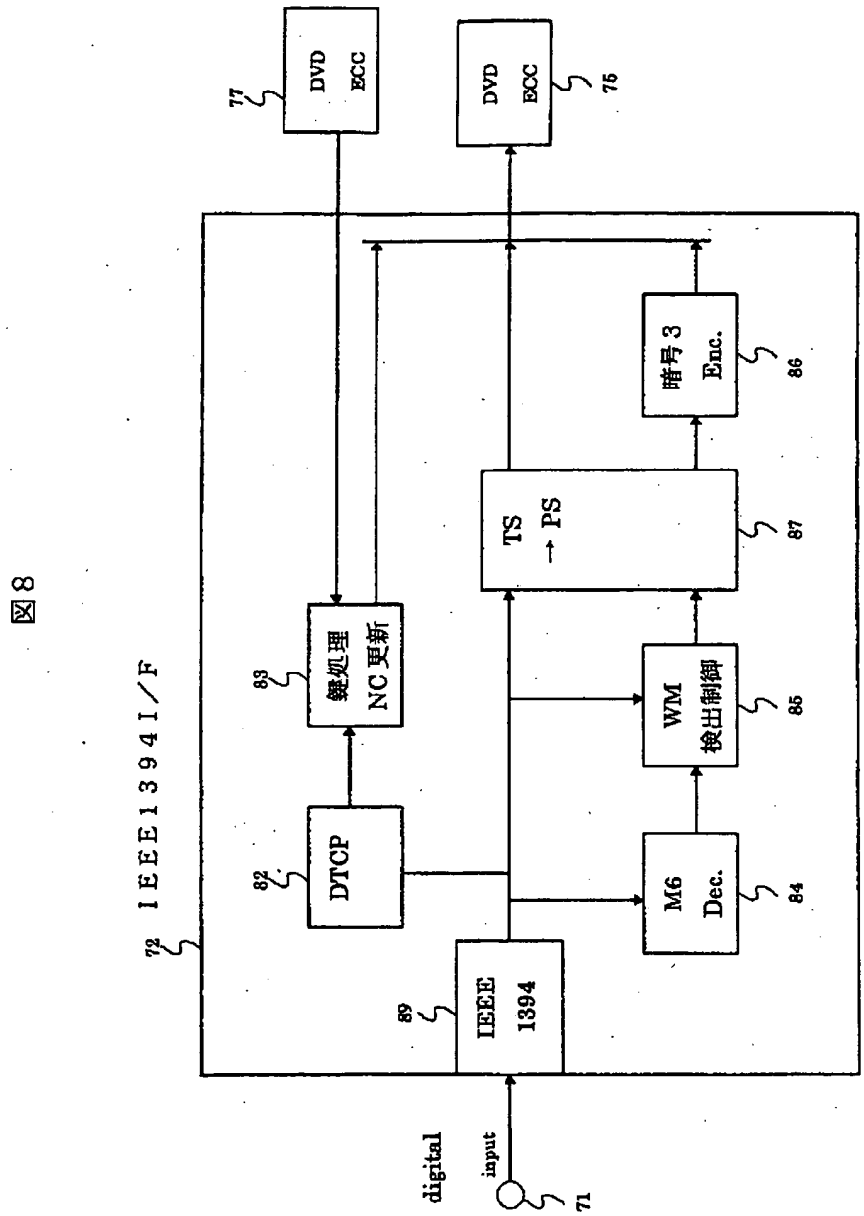

77
DVD ECC
76
DVD ECC
86
暗号3 Enc.
87
TS → PS
85
WM 検出制御
84
M6 Dec.
83
鍵処理 NC更新
82
DTCP
89
IEEE 1394
72
IEEE1394I/F
digital input
71

図8

【図９】

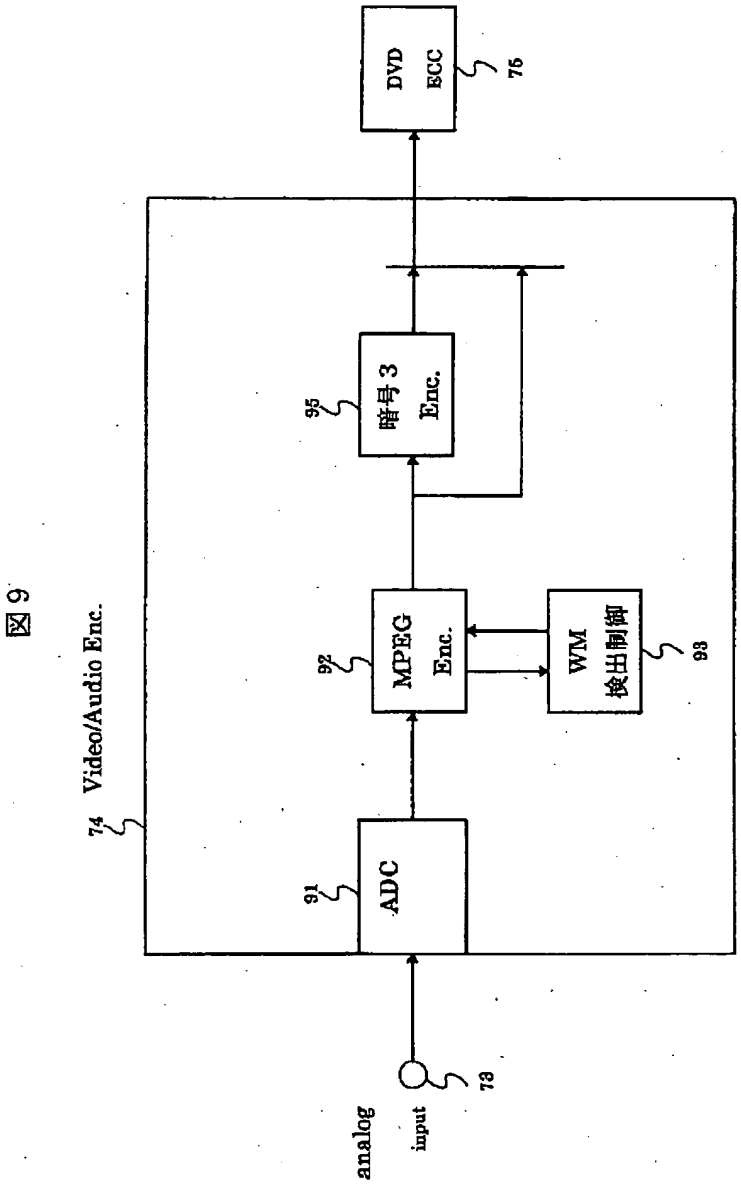

DVD
ECC
76
暗号３
Enc.
95
MPEG
Enc.
92
WM
検出制御
93
ADC
91
Video/Audio Enc.
74
analog
input
73

図９

【図１０】

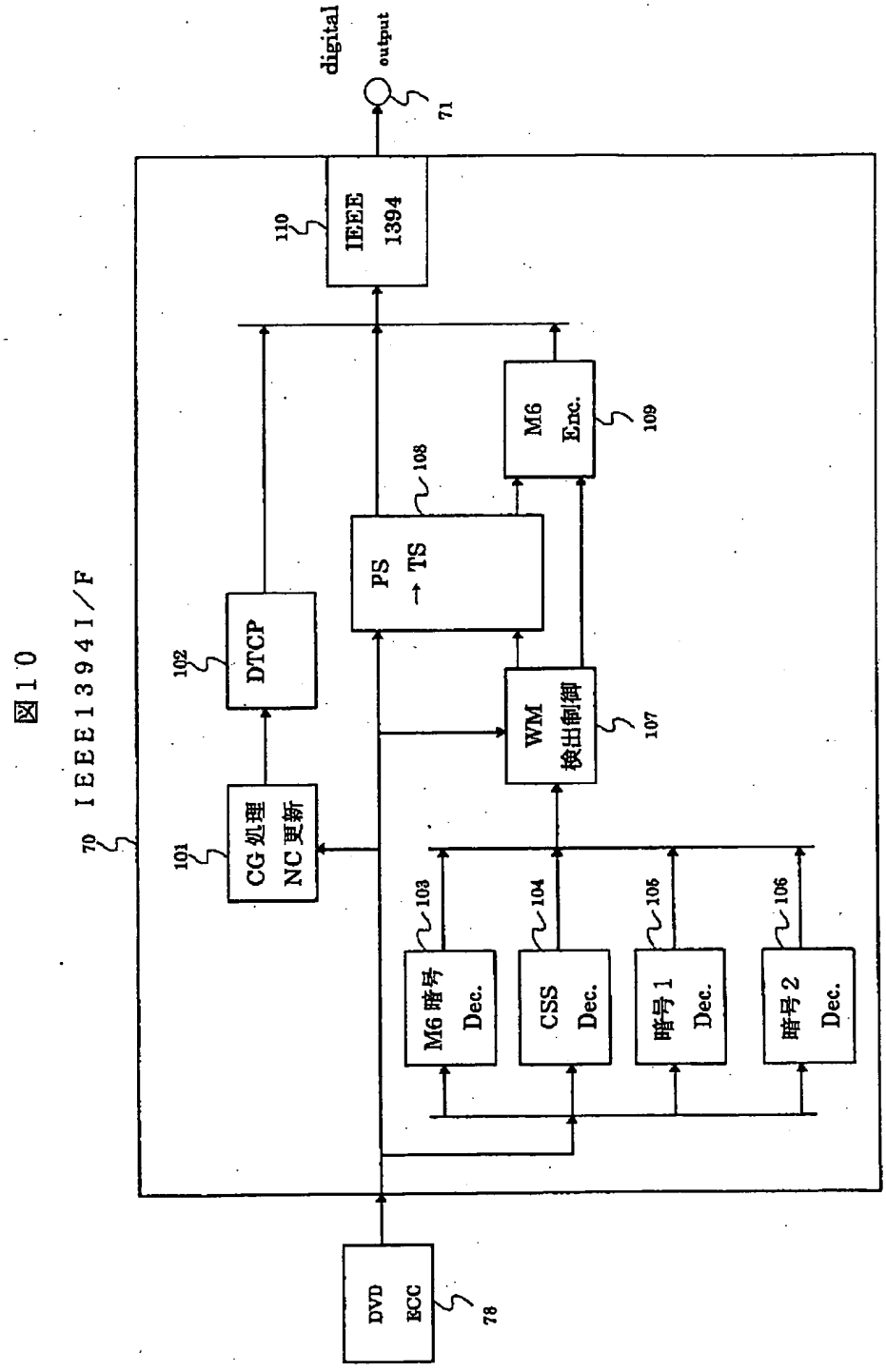
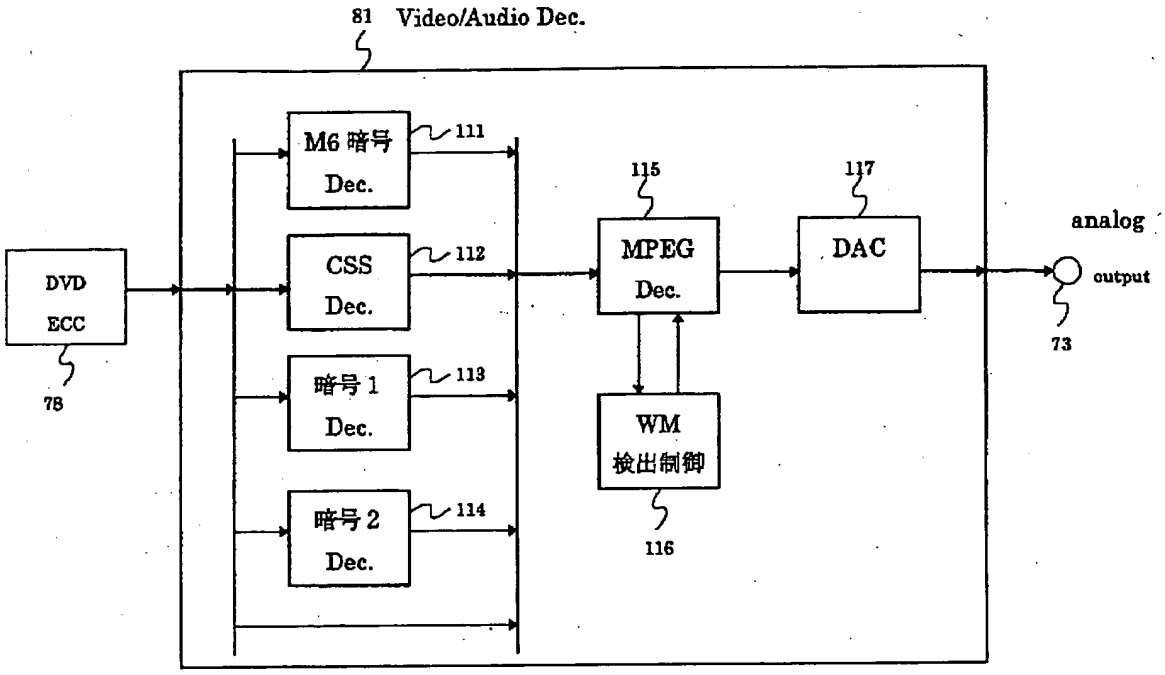

digital output
71
IEEE 1394
110
M6 Enc.
109
PS → TS
108
DTCP
102
WM 検出制御
107
CG 処理 NC 更新
101
M6 暗号 Dec.
103
CSS Dec.
104
暗号 1 Dec.
105
暗号 2 Dec.
106
DVD ECC
78
70 IEEE1394I/F

図１０

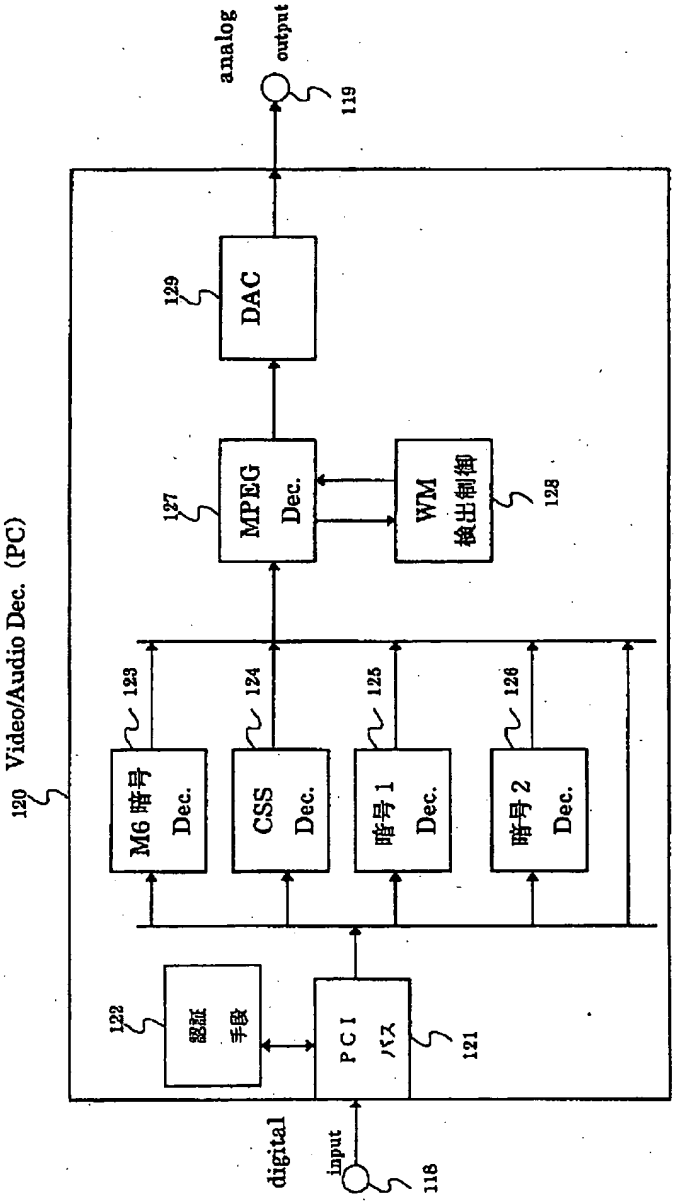
【図１１】

図１１


81 Video/Audio Dec.
M6 暗号 Dec.
111
CSS Dec.
112
暗号１ Dec.
113
暗号２ Dec.
114
115
MPEG Dec.
117
DAC
analog output
73
DVD ECC
78
WM 検出制御
116

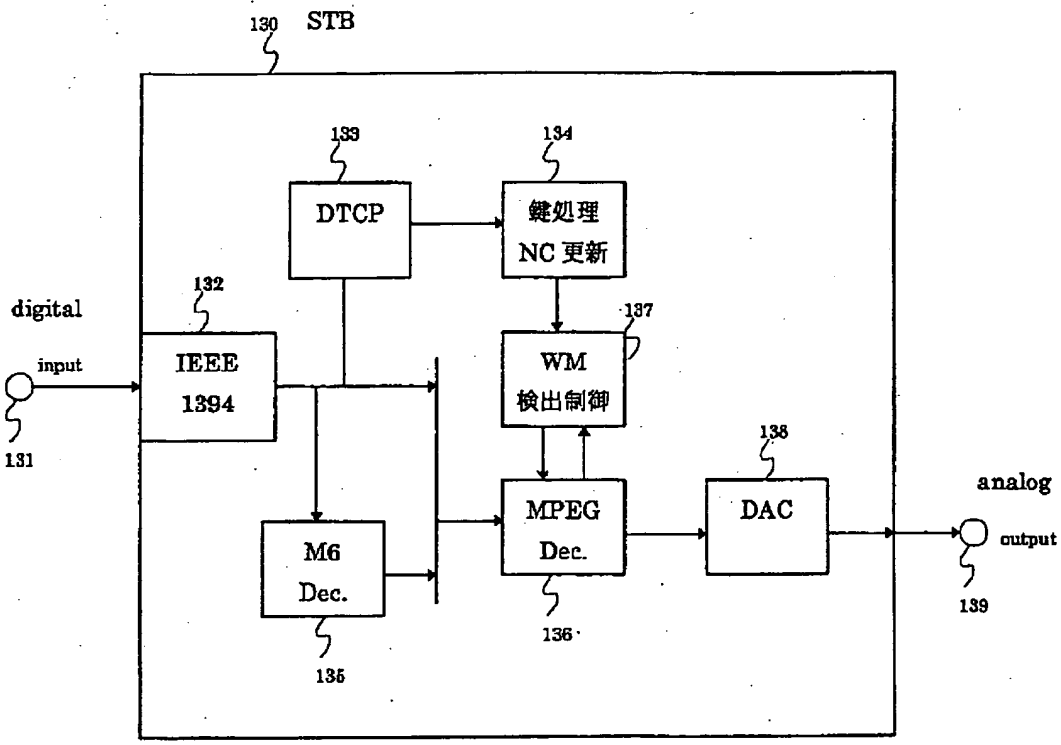
【図１２】

図１２


analog
output
119
129
DAC
127
MPEG Dec.
WM 検出制御
128
120 Video/Audio Dec. (PC)
123
124
125
126
M6 暗号 Dec.
CSS Dec.
暗号１ Dec.
暗号２ Dec.
122
認証 手段
PCI バス
121
digital
input
118

【図１３】

図１３


130
STB
133
DTCP
134
鍵処理
NC 更新
132
digital
input
IEEE
1394
137
WM
検出制御
131
138
analog
MPEG
Dec.
DAC
output
M6
Dec.
139
136
135

【図１４】

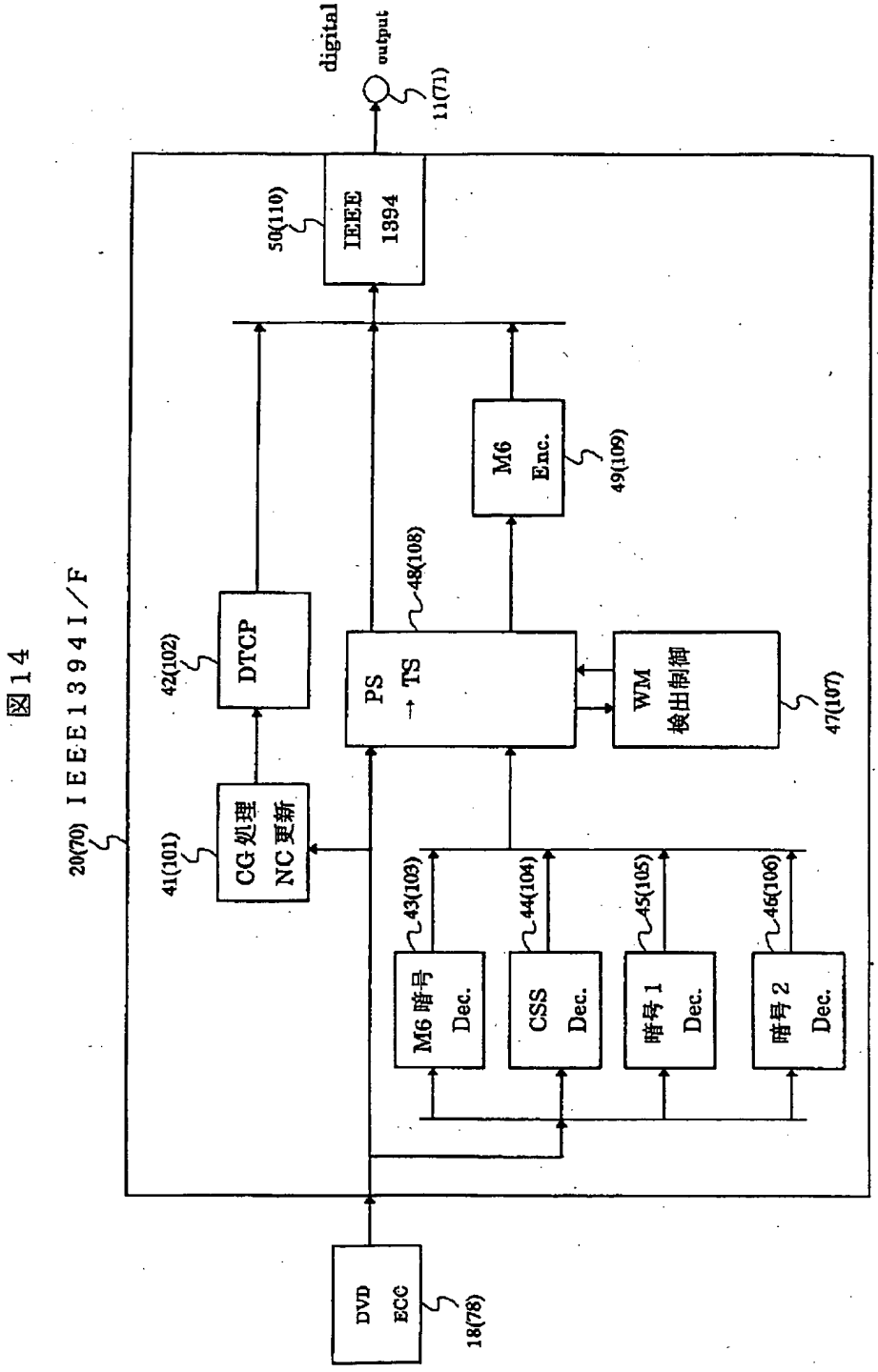

digital output
11(71)
50(110)
IEEE 1394
M6 Enc.
49(109)
48(108)
42(102)
DTCP
PS → TS
WM 検出制御
47(107)
41(101)
CG 処理 NC 更新
43(103)
44(104)
45(105)
46(106)
M6 暗号 Dec.
CSS Dec.
暗号 1 Dec.
暗号 2 Dec.
20(70) IEEE1394I/F
DVD ECC
18(78)

図１４

【図１５】

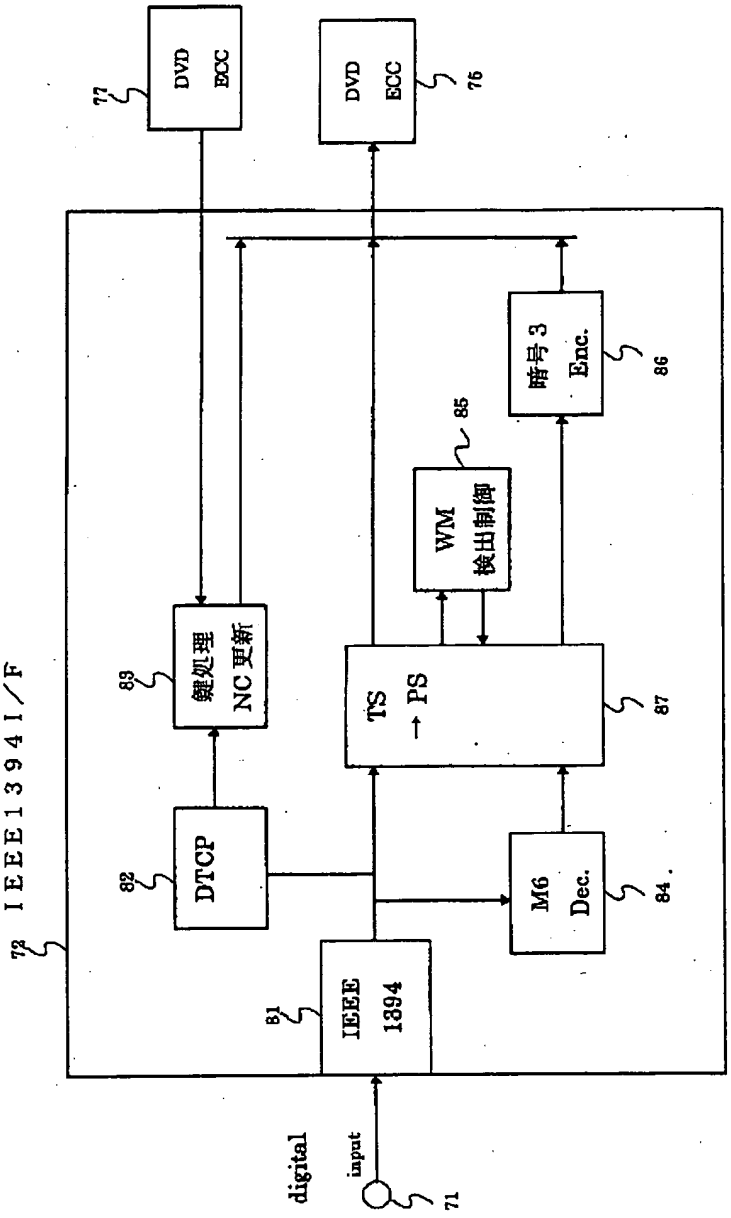


図１５

フロントページの続き

(51)Int.Cl.⁷		識別記号	FI		テーマコード(参考)
H04N	1/387		H04N	1/387	5J104
	5/91			5/91	P 9A001
	5/92			5/92	H

(72)発明者　野口　敬治
神奈川県横浜市戸塚区吉田町292番地　株式会社日立製作所デジタルメディア開発本部内

Ｆターム(参考)　5B017 AA06 BA07 BB09 CA09 CA15
5B057 AA11 BA04 CA12 CA16 CB12
CB16 CE08 CH11 DA08 DB02
5C053 FA25 GA10 GA11 GB05 GB38
HA33 JA16 KA04 KA25 LA11
5C076 AA14 BA06
5D044 AB01 AB05 AB07 BC06 CC04
DE50 EF01 EF05 FG14 FG18
GK07 GK17 GK20 HL02 HL08
5J104 AA14 JA31 NA02 PA14
9A001 BB02 BB03 BB04 CC02 EE02
EE03 EE05 HH15 HH27 JJ13
JJ19 JZ76 KK43 KK45 KK60
LL03